Security Device Roles

Vabrice Wilder
vtw3@students.uwf.edu

Abstract
"An abstract of this article was published in the proceedings of the Conference on Cybersecurity Education, Research & Practice, 2017". Communication has evolved since the beginning of mankind from smoke signals to drones to now the internet. In a world filled with technology the security of one's device is not to be taken for granted. A series of research was done in order to gather details about network devices that can aid in the protection of one's information while being transferred through the internet. The findings included but not limited to, switches, the seven layers of OSI, routers, firewalls, load balancers, proxies, web security gateways, VPN concentrators, network intrusion detection systems, intrusion prevention systems, signature based, anomaly based, and protocol analyzers. In conclusion, the findings help ensure major elements of security, which are confidentiality, integrity, and availability.

With the advancement of the internet also came the exposure of one's data and information. If one does not have a security protocol in place it then increases the risk of one's information being stolen. One of the most common security devices that individuals know is called the firewall. Firewalls are a set of hardware and software tools that monitor the flow of traffic between networks. Firewalls can regulate the connections from your network while allowing or not allowing connections based on the list of rules with which the firewall is configured.

"All people seem to need data processing" is a quick and easy way to remember the OSI model. In the application layer, one can find network application, mail, web, file transfer management, and remote connection. In the presentation layer, one can be provided a context for communication between layers, ASCII characters, encryption and decryption compression. In the session layer, one is introduced with controlling the dialogs between the computers, also controls duplexing, terminations, and restarts. The transport layer provides insight on transparent transfer of data, TCP/UCP, end-to-end connection, reliability, and flow control. The network layer is providing connection between Hosts on different networks, and IPv4/IPv6. The data link layer provides connection between host on the same network and MAC addresses. Lastly, physical layer describes electrical as well as physical specifications for device, cable, connector, and hubs repeaters.

The key elements of security are confidentiality, integrity, and availability. These terms are inextricably linked and the characteristics of the information must be protected remain the same. Commonly referred to as the C.I.A. triangle. Information that is stored on computers are almost always worth more than the computers that it runs on. Confidentiality ensures that only authorized parties with sufficient privileges may view the information. Integrity ensures that the data stored on devices is correct and no unauthorized persons or malicious software has altered data. Availability ensures network resources are readily accessible to unauthorized users.

Disciplines
Information Security | Management Information Systems | Technology and Innovation

INTRODUCTION

Security device roles contain a lot of interesting topics that fit into a secure network. While conducting research one will dive in and take a look at some of the devices, detailing how they play their part in a secure network. The three major elements of security are confidentiality, integrity, and availability. Confidentiality which ensures privacy so only the appropriate people can see the data that is important data. Integrity ensures that data has not been manipulated or changed by unauthorized people. Lastly, availability ensures you can get to your data or to your system on demand.

SWITCHES

Switches can be compared to bridges. Switches operate at layer two on the OSI model. Refer to figure 1, a OSI layer two device forwards traffic based on data link address of a device. At level two switch there is some security that can take place. For example, port security can be performed. Port security works by only allowing a certain number of MAC addresses into this port. If for example someone hooks their own switch to this port then tries to connect five or six devices those devices actually will not make it into the network. This depicts what poor security can do for one directly at the switch.

A switch might also be added by using a technique called 802.1X. For pattern purposes, 802.1X makes one prove who they are at the switch before the switch lets them traffic out to the internet. Furthermore, even come into the network. At the switch, the very first entry point for one's traffic trying to get in one must have security measurements that are conducted on a switch to control exactly who can get onto the network. If one's traffic needs to go out the web server is going to have to come off of this local network and that frame would be forwarded on to a router.

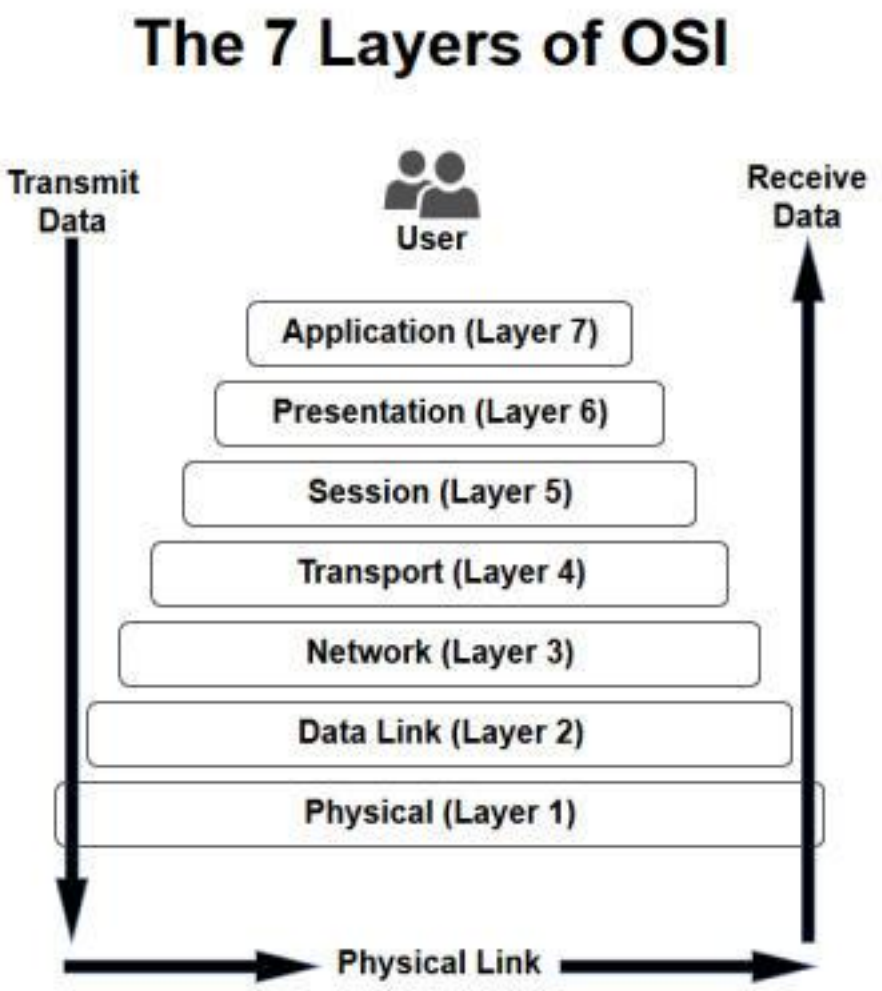

Figure 1: The Seven Layers of the OSI Model
Beal, V. (n.d.). The 7 Layers of the OSI Model. Retrieved July 21, 2017, from http://www.webopedia.com/quick_ref/OSI_Layers.asp

ROUTERS

A router is a layer three device it makes forwarding decisions based on layer three information, specifically IP addresses. Routers when making forwarding decisions for a packet, have a choice to not allow all packets through. One can have access control lists on that router to distinguish if it is going to allow packets to a specific IP address or from a specific IP address. This is what makes this router operating

at level three another point in our network where one can control traffic based on rules that are set up.

A router is a layer three device making forwarding decisions so whether it is a lowly Linux box doing routing or if it is a high-end dedicated router. One has the ability to say "yes" or "no" to certain packets based on the IP addresses involved. By default, most routers do not have any type of control list. They will simply make forwarding decisions based on what is known. One can add he access control list to the routers to help restrict what they are willing to forward. If a router is willing to forward ones packet out to the internet, one should have another device that might be in the path and that would be a firewall.

FIREWALL

A firewall also acts as a router. It makes layer three forward decisions just like a router would but the firewall has additional intelligence within. A firewall does a stateful inspection of traffic. A stateful inspection can be depicted as one's traffic going out to the internet, that traffic is meet with a firewall, and that firewall recalls in a stateful table. Some of the things that a stateful table recalls include, who the traffic came from, and what ports are involved.

If a TCP port is involved then it would track the addresses, ports, or flags at layer four. If the reply should come back from that web server the stateful firewall begins a recalling process. The firewall as shown in figure 2, usually does not allow traffic from the internet into its internal users recalls. It begins to recall if a specific user's connection was in its stateful table and ensures the reply is accurate. After remembering and ensuring, it then allows return traffic to come back in.

So, a firewall looks at layer three information, to ensure it is looking at layer four information, and maybe searching even higher in the protocol stack. By doing this a firewall can make its decision to allow return traffic to come back in. If an attacker tries to initialize a connection going into a firewall by someone it would be able to recognize that it does not have a request from said person going out. By the firewall doing this it does not allow the initial request for the attacker to come into someone's network. An example of this could be a dedicated firewall device, such as Cisco, a checkpoint, or/and a Linux box.

There could be a benefit of having a router and a firewall. The router can do certain functions and the firewall do other functions. It is possible to have a single device that does all routing and contains all firewall stateful inspection on one device. If someone is trying to reach the Google engine there is not just one

physical server that supports the entire planet. The Google engine server spits up the load with a technique called a load balancer.

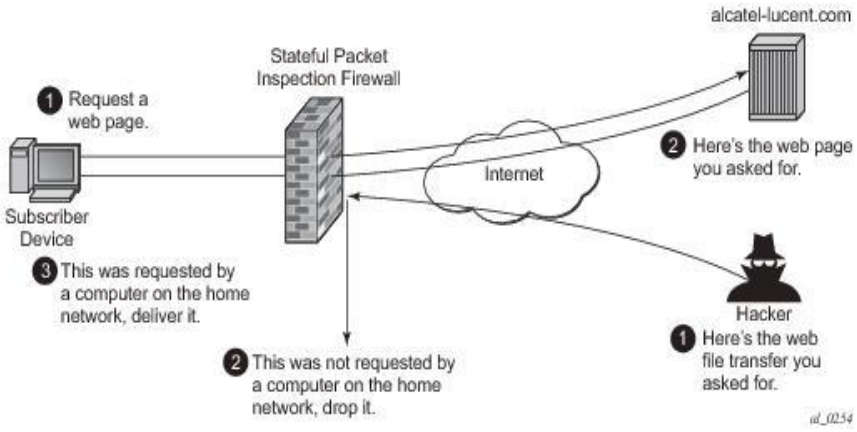

Figure 2: Block Unsolicited Traffic

Application Assurance — Stateful Firewall. (n.d.). Retrieved July 20, 2017, from https://infoproducts.alcatel-lucent.com/html/0_add-h-f/93-0267-HTML/7X50_Advanced_Configuration_Guide/AA-FW.html

LOAD BALANCER

We can use Googles servers to give us a clear example of load balancing. For example, Google has four servers all which run the same content. All four servers hide behind a single IP address. Someone does a DNS request for Google than receives one or more IP addresses. When it reaches an IP address, that specific IP address could be the front end for multiple servers. Every request could go to different servers. It could use round robin or use the least used server at the moment. Availability is involved in the load balancer process when one has resources that it needs access to. A load balancer in this case can increase the availability, especially if there is a large quantity of requests for a specific resource.

The key to the load balancer is dividing traffic across multiple devices. The benefits of having a load balancer is availability. Take for instance, if there is an overload of traffic headed to a resource. A load balancer will split the load across multiple devices. The availability of the response from those servers is greater. Also, if a device fails and the load balancer is no longer getting a response from that device it can still perform load balancing on the remaining three servers. All in all, whenever there is a need for high availability for a given resource on the

internet usually a load balancer is involved that can keep that availability for that resource.

PROXIES

To ensure people do not go to websites they are not permitted to a proxy server is an option to regulate. A proxy server redirects web traffic. A benefit of a proxy server is that it can look at all the information in the protocol stack, monitor, and limit access to websites. It does this because the entire session is going to the proxy server. A proxy server has an opportunity to take a in depth look at all the details at the application layer. At the application layer, it monitors and filters. Filtering can be called URL filtering or content filtering depending on one's vendor and the implementation. Some of the things a proxy server might look at include, what websites one is trying to access. Rules can be drafted on a proxy server that specify what type of websites are not allowed or what URLs are not allowed. Proxy serves usually use some kind of third-party service.

WEB SECURITY GATEWAYS

A web security gateway depends on the vendor and the features. There is a firewall that has the ability to take a glance at the application layer to view what is going through. If one decides to use HTTP's to access some web resource. The device that can be used is web security gateways. Web security gateways can look at things like, are these valid HTTP's requests, the content, and the tags involved inside of that application. Web security gateways has the ability to depict if there is something harmful happening.

Web security gateways has the ability to see if there is improper HTTP commands or HTTP syntax. A web security gateway looks at the HTTP information at the application layer. A web security gateway identifies based on how the vendor implements a solution and then stops it from occurring. By a web security gateway stopping the vendor implements, a firewall determines by looking at both sides that the session needs to end. This can be defined as application aware or layer seven firewall. Again, these devices can look at the upper layers of a protocol stack to observe what the application is doing.

VPN CONCENTRATORS

"A virtual private network (VPN) is a constructed used to provide a secure communication channel between users across public networks such as the internet" (White,2015). VPN tunnels which is a virtual private network, uses

cryptography and encryption for confidentiality. VPN concentrator is a dedicated device that manages multiple VPN's tunnels. If the users authenticate and prove who they are then the VPN concentrator allows traffic into the network. "VPN concentrator come in a variety of sizes, scaling to enable VPNs from small networks to large. A VPN concentrator allows multiple VPN connections to terminate at a single network point" (White, 2015).

N.I.D.S. AND N.I.P.S.

Another challenge that networks face is malicious traffic that is going over the network. Identifying and stopping this malicious traffic can be done by putting a device on the network called an intrusion detection or an intrusion prevention system. Network intrusion detection systems can see the traffic. NIDS can set off alarms but it cannot stop the traffic. NIDS is more of a warning system. Network intrusion prevention systems can also see traffic. IPS also has alarms that inform when something is off, but it has the ability to stop the traffic before it enters the network. A benefit of using a network-based intrusion detection system or intrusion prevention system is one can monitor the traffic to websites, the entire company, or subnet. As opposed to a single device at a time. The option to monitor a single host is a host-based IDS or host based IPS.

SIGNATURE BASED

A signature based knows whether or not traffic coming in is good or bad. A signature base method that an IDS or IPS system uses is definition based. A reason for this method may be because a signature based IDS or IPS has a database of specific things that it is looking for. For example, if there is a vendor like checkpoint that has two thousand signatures in their database. All the traffic that is going through the network is being compared against those two thousand signatures.

If there is a match then there is an alarm that is activated. Then based on the rules that are set up: If IPS device it may decide to proceed and stop the traffic from entering the network. If IDS device it can fire off on that signature, send an alarm so that one can be notified that there is activity is happening on the network. Signature-based is only going to fire off or identify known attacks that match one or more of the signatures in the signature database of the vendor whose IPS or IDS one is using.

ANOMALY BASED

Traffic that is not in the signature database, still may contain a problem for a network. We can use behavior based which can also be thrown into a category of anomaly based and heuristics. If for example, one plugs in an IPS or IDS device into a network and it dynamically looks at all the traffic. It might gather a baseline. One primarily method that is used with an anomaly based is with TCP scans.

If a client is going out and looking for resources it sends a TCP SYN/request and it should receive a SYN/ACK coming back. An anomaly based system could keep track of the average number of half form sessions at any given time. If the number is five, for example, we have five half form sessions at a time and that is the baseline. Then it can go up to a hundred or thousand which is very indicative of something like a worm or some other attack that is happening with TCP scans across one's network. The anomaly based system says here is the baseline of five.

So, anomaly based IPS does not need a signature to match on. The anomaly based is looking for some type of anomalous traffic pattern compared to the baseline. Furthermore, a lot of times when one gets an IPS or IDS system they may put it in IDS mode. This is for the system to passively learn the network to build its baselines without taking action. Once everything is understood to reduce and minimize false/positives of that system then, one might turn on IPS mode. One might turn on IPS mode because now it is known what their baselines is and what alarms will be firing off after they have tuned it for their specific network.

PROTOCOL ANALYZERS

On a network if there is malicious activity or if one wants to know any basic information on a network segment the usage of protocol analyzer is a solution. Protocol analyzer actually has several different names. A sniffer is one name for protocol analyzer, it looks through packets and frames. Then presents the information in a graphical user interface detailing each and every part of those packets. If one wanted to look at all the traffic for example, between an interface of the router and this interface of the firewall we could put a protocol analyzer in use.

One can take a look at the details on that network segment and find all types of interesting things. Such as, a lot of fragmentation that is happening, flooding that may be occurring, or protocols one might not have known existed running on our networks. If there is a problem one can use a protocol analyzer to help identify what the problem is. A protocol analyzer actually monitors the play by play on the network. A protocol analyzer helps identify a problem between two

devices or two applications that are communication or should be communicating. Another reason why it is important to have a baseline, so one knows the normal patterns of its network. A protocol analyzer can also help us identify what is truly happening within one's network.

REFERENCES

[1] Conklin, W. A., White, G., Cothren, C., Davis, R. L., & Williams, D. (2015). *CompTIA security: exam guide (exam SYO-401)*. New York: McGraw-Hill.

[2] 02 Network Security Devices. (2016, December 22). Retrieved July 18, 2017, from https://www.youtube.com/watch?v=mt1CaCD6Tto

[3] Day 30. Networking Models and Data Flow. (n.d.). Retrieved July 19, 2017, from http://ptgmedia.pearsoncmg.com/imprint_downloads/informit/learninglabs/9780134213736/ch30.html